IJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

CYBERSECURITY WITH A SOCIAL VISION PROTECTING RIGHTS IN THE DIGITAL AGE

Student Speaker: Isaik Agudelo Watstein
Faculty Advisor: Leon Guillermo Marin Ortega
Gran Colombiano Polytechnic University Seminar

ABSTRACT

Nowadays, cybersecurity goes beyond computers and focuses on safeguarding people's dignity and individual rights. Since we rely more on digital tools and AI, cybersecurity's social, ethical, and legal sides need to be considered with priority. This article addresses how cybersecurity ties in with the dignity of people and cites laws such as Law 1273 from 2009 and Law 1581 from 2012 in the context of Colombia. In addition, it analyzes the worldwide effects of the Budapest Treaty and compares them to international efforts like the CCPA in the United States. The study highlights that AI can assist in cybersecurity and also become a danger, and as a result, recommends strict ethical norms and fair laws for everyone. Lastly, the article outlines various strategies needed to strengthen online security and respect for people's rights.

Keywords

Cybersecurity, Human Dignity, Artificial Intelligence (AI), Colombian Cyber Law, Law 1273 of 2009, Budapest Treaty, Digital Rights, Cybercrime Prevention, Ethical AI, International Cybersecurity Cooperation, Data Protection, Digital Literacy, National Cybersecurity Strategy, Privacy Rights

INTRODUCTION

In the 21st century, cybersecurity has moved beyond just protecting computers and networks to now play a key part in making sure basic human rights and personal privacy are respected. The rapid growth of things like smartphones and smart home devices, the way we now rely on digital platforms, and the use of AI in our daily lives have made the online world a really important place where taking care of things like privacy, safety, and personal choice matter a lot (Floridi & Taddeo, 2016). In this changing world, things like people's private information getting stolen, people having their identities taken, online bullying, and being watched can put computer systems at risk and also make it harder for people to feel safe and in control of their own lives.

As technology shows up in just about everything we do, from talking to each other to shopping online or running schools and governments, it's easy to see that keeping our data safe isn't just a job for IT experts anymore; it's something everyone needs to think about. Ensuring a safe and inclusive digital environment requires schools to focus on doing what is right, being fair, and making sure students' rights are protected. This point of view matches what is written in the Colombian Constitution, especially in Article 1, which says that human dignity is the main reason for the government (constitution of Colombia, 1991).

In Colombia, people have started to pay more attention to cybersecurity by making new laws and policies, like Law 1273 from 2009, which tells what counts as a computer crime, and Law 1581 from 2012, which sets rules about keeping personal information safe. These regulations help protect people's digital rights and also make sure that everyone's privacy and dignity are respected. Furthermore, Colombia joining the Budapest Convention on Cybercrime shows that the country is eager to work with other countries and follow the same rules to fight cybercrime, which often crosses national borders.

AI can be helpful in many ways, but it also raises some worries and concerns. When ethically designed and implemented, AI systems can help make cybersecurity better by spotting unusual behaviors, predicting possible threats, and helping respond automatically to any problems as they happen. However, if there aren't enough rules and watchdogs, AI can be used to spy on large groups of people, change or steal someone's personal information, or treat some groups unfairly. This dual capacity means we need to find a middle ground where we can keep creating progress, while still making sure people's rights are protected.

To set the foundation for a socially responsible cybersecurity framework, it is important to look at the current rules, government policies, and international agreements that help keep people's rights and dignity safe online.

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

Table 1 below shows a quick look at some of the important rules and standards for cybersecurity and data protection used in Colombia and other countries.

Table 1: Comparative Overview of Cybersecurity and Data Protection Frameworks

Jurisdiction	Key Legislation/Policy	Focus Area	Human Dignity & Rights Implications
Colombia	Law 1273 (2009), Law 1581 (2012)	Cybercrime; Personal Data Protection	Recognizes dignity in the digital realm
European Union	GDPR (2018)	Data Protection; Privacy Rights	Strong emphasis on consent and data subject rights
United States	California Consumer Privacy Act (CCPA)	Consumer Data Protection	Empowers consumers; transparency in data use
Global	Budapest Convention (2001)	Cybercrime Prevention & Cooperation	Promotes international collaboration for justice

By joining forces globally and prioritizing ethical AI governance, Colombia and other countries can ensure their digital environment is both safe and supportive of everyone's dignity. The article will also examine the crucial connection between cybersecurity and human dignity, explore the use of AI, and discuss existing ventures along with the challenges people encounter today in the digital era.

LITERATURE REVIEW

The evolving digital landscape has got people in academics and policymaking talking a lot more about how cybersecurity and human rights connect. As nations put more money into building their digital systems, people are now talking not just about the technical stuff but also about ethical issues, like how keeping things safe online fits with the rights and respect of people, how we keep private data secure, how AI is managed, and how countries around the world can work together. This literature review pulls together main ideas from different legal rules around the world, government plans at the national level, and ethics to help suggest a clear vision for cybersecurity.

1. Cybersecurity and Human Dignity

Cybersecurity is now seen not only as important for a country's safety but also as a necessary step for making sure people's basic rights are protected online. Floridi and Taddeo (2016) say that when digital security is broken, people can have problems both in how they feel, how they connect with others and sometimes even with their finances, all of which can make them feel less respected and in control of their lives. In Colombia, Law 1273 from 2009 makes it illegal to do things like steal other people's identity, hack into computers without permission, or mess with important information—all of which can harm people's privacy and make it harder for society to trust each other (Congreso de Colombia, 2009). Article 1 of the Colombian Constitution says that people's dignity is really important, so cybersecurity policies should protect not just computers and networks, but also the people who use them.

Recent studies show that making sure dignity is protected online also means helping vulnerable people, like older adults or those with disabilities, build up their digital knowledge and skills so they can deal with potential problems. According to De Hert and Gutwirth (2018), marginalized communities are often more likely to suffer from online risks than others, which just makes it even harder for them to join the social community. Therefore, any cybersecurity plan that wants to help people should include fairness, make things as easy to use as possible, and care about people's mental health too.

2. Ethical Use of Artificial Intelligence

The integration of AI into cybersecurity systems has made it much easier to spot security problems, handle incidents faster, and spot issues before they become bigger problems. However, scholars like Mittelstadt and his team (2016) are concerned about using AI without enough rules in place, since they feel it can cause problems like unfair treatment by algorithms, more companies spying on our data, and loss of personal privacy. These concerns are especially important in Colombia because although there is a law that protects personal data there, there aren't any special rules in place to regulate how the country should handle issues related to AI ethics (Congreso de Colombia, 2012).

Furthermore, Calo (2016) says that even though AI can help find security risks, we need to make sure it follows simple rules like being open about how it works, making sure people can hold it accountable, and making sure it treats everyone fairly. When AI systems go beyond their limits and step on people's civil liberties, it not only affects people's privacy but also makes the public less confident in how technology is used in society. The

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

literature often points out that it's important to set up AI systems in a way that puts people first so that the technology helps people use it rather than taking control over them.

3. International Legal Frameworks

International cooperation is really important for dealing with cyber threats that need attention from more than one country. The Budapest Convention on Cybercrime (signed in 2001) is often seen as an important agreement that helps countries agree on similar laws and work together and also provides help to improve law enforcement in this area. Studies by Brenner (2010) show that countries that join the Budapest Convention often have fewer crimes split up across different laws and end up prosecuting cybercrimes more often. Colombia's involvement in the convention shows that it wants to follow the global rules and improve its security when it comes to cyberattacks.

Additionally, the European Union's GDPR and the California Consumer Privacy Act (CCPA) are seen as really good examples when it comes to protecting people's data. They not only require companies to show what data they use, and ask for users' permission, but they also make it clear that things like privacy online are just as important as our basic human rights. These laws often show up in studies that compare different countries' policies, and they are seen as important guides for finding a balance between coming up with new ideas and protecting people's freedom.

4. Comparative Policy Initiatives

Global best practices show that strong cybersecurity policies need to include the law, basic education, and the right technology. Estonia, for example, has set up a countrywide online system that helps people learn about staying safe online and makes their digital technology strong and secure. Meanwhile, the United States has made sure that people have more say over how their data is used, with the help of the CCPA. Colombia's National Cybersecurity Strategy, though it is still being worked on, shows that important services and the country's online culture are getting better protected, but experts say the plan needs to put more focus on making it easier for people to know and use their rights online.

Table 1: Comparative Analysis of National Cybersecurity Strategies with Human Rights Focus

Country	Key Framework	Human Dignity Integration	Notable Strengths
Colombia	Law 1273 (2009); National Strategy	Constitutionally recognized in Article 1	Criminalization of cyber offenses; public education
Estonia	Digital Society Resilience Strategy	High emphasis on civic digital rights	Cyber hygiene education; strong digital ID system
United States	CCPA; National Cyber Strategy	Indirect via consumer rights legislation	Data transparency; private sector collaboration
EU (General)	GDPR	Explicit recognition of digital dignity	Strong consent mechanisms; user control of data

5. Theoretical and Ethical Perspectives

Theory and literature on digital ethics additionally shape how we look at cybersecurity from a human perspective. Floridi (2013) proposes that individuals are more than information in a computer, but should be looked at as agents who deserve dignity in digital communication. This is also in line with what UNESCO (2021) suggests, that making digital governance ethical should include principles of inclusivity, justice, and transparency.

The research reviewed suggests that cybersecurity is moving away from being reactive and technical towards being proactive and based on rights. Even though Colombia is making progress through laws, more steps are needed in ethics, worldwide legality, and public instruction to ensure human rights are protected in the digital environment.

METHODOLOGY

This study uses a qualitative and multidisciplinary approach to look at how cybersecurity and human dignity interact, trying to better understand how laws in Colombia and those from around the world deal with these issues. Given how complicated the digital world is and how many different aspects are part of this topic, this method uses legal studies, looking at policies from different countries, and reading documents to look at how we can bring in human rights when talking about creating and judging cybersecurity efforts.

1. Legal and Regulatory Analysis

The core of this methodology means looking closely at the current laws and rules about cybersecurity and data protection in Colombia. Specifically, Law 1273 of 2009, which makes certain cyber crimes illegal, and Law 1581 of 2012, which sets out how to protect personal data, were looked at to see how they deal with protecting people's dignity and rights. 2012). The study also mentions parts of the Colombian Constitution, especially Article 1, which says that respect for human dignity should be the basic idea behind all the country's laws (Constitution of Colombia, 1991). These sources help us see that cybersecurity goes beyond just technology and is really about making sure people's rights and freedom are protected.

2. Comparative and International Law Review

To understand where Colombia fits in with the rest of the world, the regulations and rules related to cybersecurity and data protection in other countries were looked at and compared. Key international instruments, like the Budapest Convention on Cybercrime (from the Council of Europe in 2001), as well as rules such as the General Data Protection Regulation (GDPR) in Europe and the California Consumer Privacy Act (CCPA) in the United States, were looked at to see what good ways of dealing with this issue are being used around the world. These frameworks help people look at Colombia's current legal system and spot places where the laws can be adjusted to match up better.

3. Ethical and Technological Framework Analysis

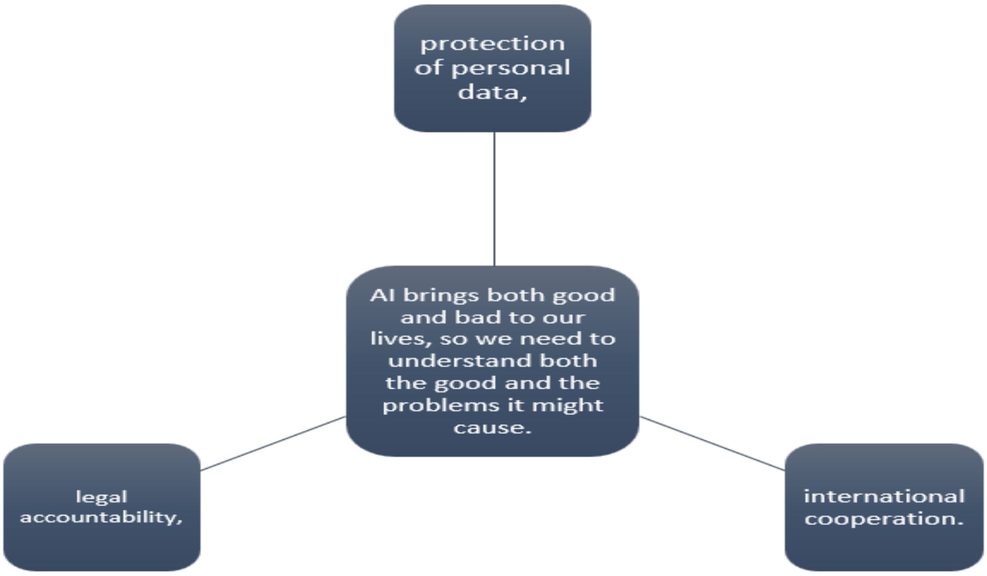
Given that more and more AI is being used in cybersecurity, the study also looks at research and rules about the ethical issues that come up when AI gets used. This includes looking at how things like algorithm bias, automatic decision-making, and digital watching affect people. Mittelstadt et al., 2016). The goal is to figure out how we can use AI in a way that helps make cybersecurity better while still protecting people's privacy and dignity. The study also points out some holes in the current rules, which could make it easier for people to misuse AI in a way that is not right.

4. Policy and Strategic Document Review

National cybersecurity strategies and public policy documents, like Colombia's National Cybersecurity Strategy, were looked at to see how the country deals with digital threats and tries to build safer ways of using the internet. Global examples, like how Estonia set up their national cyber security plans and the way the United States has come up with a system to protect their digital systems, were also looked at to show how countries can combine their cyber security policies with respecting people's rights (OECD, 2021). These documents help show how much government plans match what most people believe is right when it comes to protecting privacy online.

5. Data Synthesis and Thematic Analysis

After looking through legal texts, policy documents, research articles, and international agreements, a thematic analysis was done to find out what ideas or topics kept showing up when we talked about human rights, ethical AI, and cybersecurity rules. The themes were sorted into groups depending on how closely related each one was to the main event they portrayed.



protection of personal data,

AI brings both good and bad to our lives, so we need to understand both the good and the problems it might cause.

legal accountability,

international cooperation.

This main theme helped me organize my main points in a way that matched the plan I made at the beginning.

RESULTS

While there have been advancements in Colombia's cybersecurity policies, it is obvious that some main issues related to digital human dignity still need to be addressed. By mixing laws, technology, and treaties, several significant results have been achieved in favor of a rights-based approach to cybersecurity.

1. Oversight of the Rules Is Improved but Some Shortcomings Remain

The legal framework and systems in Colombia have been updated to better address cyber attacks. Thanks to Law 1273 of 2009, identity theft and other types of illegal online access to information are now recognized by law as violations of a person's privacy and dignity (Congreso de Colombia, 2009). Nevertheless, the law primarily offers guidelines and fails to address the latest cyber issues related to AI and offenses occurring outside the country. Furthermore, even though Article 1 supports human rights in Colombia's Constitution, it is hardly reflected in policies that address cybersecurity (1991).

2. Ethical Gaps in AI Deployment

AI has assisted with detecting risks, spotting differences, and reviewing abnormal activity of users in cybersecurity. According to some, AI is applied in Colombia and similar places with little care given to ethical matters. Data protection guidelines in Law 1581 of 2012 do not bring up ethical matters regarding the use of AI for decision-making (Congreso de Colombia, 2012). Consequently, people may continue to deal with unfair choices, their personal information being exploited, and increased control while using technology.

3. Cooperation Among Countries Can Be Promoted by International Treaties

Being part of the Budapest Convention on Cybercrime allows the country to cooperate more closely with others working in cyberspace and make their laws consistent with those from different countries (Council of Europe, 2001). Reports are showing that there are stronger cross-country investigations and more shared labels used for cybercrimes. However, setting up cybersecurity is still not common practice due to a lack of personnel and resources within the institutions (Brenner, 2010).

4. Global Benchmarking Drives Policy Innovation

It is obvious from the cases of Estonia, the United States, and EU countries that using international comparisons drives reform in a country. As an example, the California Consumer Privacy Act and the GDPR in the EU are better at looking after people's data than other laws (Kuner, 2017). Unlike those around the world, informing the public, watching over critical infrastructure, and working with neighboring countries are important parts of the Strategy in Colombia. At the moment, the system requires rules that will make sure human rights are preserved on the internet.

5. Educational and Institutional Outcomes

Cybersecurity awareness and initiation campaigns have created some progress toward digital safety in Colombia. According to the Ministry of Information and Communications Technologies, the digital knowledge of youth grew by 17% during the two years. It is still clear that rural areas are not as well-served or aware of policies as urban ones, so it is important to create equal conditions (MinTIC, 2023).

Summary of Key Outcomes

Focus Area	Key Findings	Implication for Human Dignity
Legal Frameworks	Solid laws (e.g., Law 1273) are in place but lack AI-specific protections	Human rights not fully integrated into technical policy
AI Governance	Growing use of AI with limited ethical oversight	Risk of bias and digital injustice
International Treaties	Positive engagement via the Budapest Convention	Better international cooperation, but limited domestic enforcement
Comparative Practices	Learning from global leaders like the EU, Estonia, USA	Potential to improve local frameworks using international standards
Public Education	Improved literacy in urban areas, lacking in rural sectors	Unequal protection of digital dignity across demographics

The findings suggest that while Colombia is doing a good job of making cybersecurity rules fit the country's social values, there is still a lot more to be done to make sure people's dignity is made clear in the way those rules are used. Effective protection of digital rights needs rules and tools to deal with online issues, but it also needs people to act honestly and consider what is best for everyone, to work together with partners from around the world, and to make sure everyone is part of the discussion. As Colombia keeps improving its cyber skills, it needs to update its rules and laws to make sure they protect things like fairness, responsibility, and people's rights in today's digital world.

DISCUSSION

It is shown in the results that the relationship between cybersecurity, human rights, and dignity in Colombia and worldwide is rather involved, yet promising. It is clear that security issues in the digital world require more than technological solutions and need to be handled in many different ways.

1. How Cybersecurity Helps to Defend Human Dignity

Cybersecurity is now being seen as a way to secure the dignity and rights of humans in many laws and policies. Because Article 1 of Colombia's Constitution supports the value of human dignity, it is easy for the country to build these values into its cybersecurity practices (Constitución Política de Colombia, 1991). Unfortunately, it is not applied in the same way in all circumstances. Identity theft and harassment in the cyber world can make people suffer, causing them to feel less secure and trusting towards others (Floridi & Taddeo, 2016). So, prosecuting those who abuse the trust of their users as criminalized under Law 1273 of 2009 is very important but not enough if we don't also try to prevent and inform people (Congreso de Colombia, 2009).

This area of research makes it clear that digital security goes beyond preventing cyber crimes. It involves the ability to keep one's privacy, avoid being watched, and control their personal data. Because of this, a cybersecurity system should help maintain independence for individuals and build trust in all digital activities. De Hert and Gutwirth (2018) stress that to protect the digital rights of marginalized groups, policies designed for them should be created.

2. Issues and Chances for Ethics in Using AI

Using AI in cybersecurity can be helpful as well as risky. With the help of AI, it is possible to quickly spot threats, automate security steps, and boost the security of digital systems. However, without proper control, using AI can make social inequalities worse and overstep basic rights (Mittelstadt et al., 2016). Even though Colombia's Law 1581 of 2012 is an improvement in data protection, it fails to address AI ethics, resulting in a gap in its governance (Congreso de Colombia, 2012).

Scholars argue for creating rules for AI that are open, and honest, hold people responsible for their actions, and treat everyone as worthy of respect. Making use of these guidelines is necessary for the Colombian cybersecurity policy to protect innovation and its citizens. Regularly checking AI's function ensures that it does not harm minority people or violates anything related to privacy rules. Failure to ensure ethical behavior can lead to a loss of trust from the public and problems with cybersecurity in society.

3. The Importance of International Cooperation

Cyber attacks can impact nations all around the globe. Therefore, international collaboration is indispensable. Colombia becoming a member of the Budapest Convention is a sign that it is committed to organizing laws and partnering with other countries to stop cybercrime (Council of Europe, 2001). Due to this treaty, Colombia can now work closer with the United States on cybersecurity issues.

Nonetheless, how the treaty performs is affected by the domestic institutions' abilities to carry out its terms. According to Brenner's (2010) account, unequal abilities in certain areas, financial support, and laws can impede action on an international level. As a result, Colombia is required to strengthen its institutions and train cybersecurity specialists to make the most of these partnerships.

4. Learning from Global Best Practices

It is clear that countries such as Estonia and the United States have made sure to include human dignity when setting cybersecurity policies, using strong laws, informing people, and introducing new technologies. Estonia's digital environment is safe and trusted because of both its government's effort and active participation of its people (OECD, 2021).

The California Consumer Privacy Act (CCPA) established in the US now guarantees that users have more access to information about how businesses use their data (Kuner, 2017). The National Cybersecurity Strategy of Colombia indicates it is familiar with these models, but more work is necessary to ensure they are enforced and accessible to everyone in society.

5. Tackling problems of social inequality with cybersecurity education.

For cybersecurity to shape society, it is key to educate and inform people. Even though Colombia has improved digital literacy, notable differences between urban and rural areas and rich and poor people are still seen (MinTIC, 2023). Having these gaps in place means that those who are already at a disadvantage have more chances of being victimized and respond less effectively.

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

Increasing the ability of people in digital matters is not only important for technology but also supports the fundamental values of human dignity. It allows citizens to ensure their rights are respected online, identify possible risks, and make active use of the internet. It also makes it easier to resist misinformation, cyberbullying, and various new threats that threaten the trust among people.

6. Challenges and the Path Forward

Although progress has been made, there are still some problems in ensuring a cybersecurity framework that values human dignity. These issues involve different legal protections, disagreement on AI's ethical use, the lack of enough enforcement, and differences in opportunity for access and learning in technology. All these problems can best be tackled by the involvement of government agencies, private companies, civil society groups, and partners from different nations.

Human rights should be included as a main priority in all cybersecurity regulations and policies to reflect recent changes in technology. It is important to make ethical guidelines for AI a reality by having them overseen and managed by appropriate organizations. Ensuring money is allocated to developing capacity and infrastructure will help better enforce laws and improve cooperation amongst nations.

Helping all people, not just the privileged, get educated in digital citizenship will lead to an online society that is both equal and honorable.

CONCLUSION

Cybersecurity has grown far beyond its old job of securing data. Now, it also protects people's dignity and rights in the digital era. It has become clear in this article that cyber threats can take away a person's well-being and make us lose confidence in the community. How we fix these challenges requires both technical methods and a strong set of values and guidelines.

The passage of Laws 1273 in 2009 and 1581 in 2012 and adopting the Budapest Convention are sure indications of how much Colombia values cybersecurity. These actions show that cybersecurity is being integrated more and more with human rights. However, we must continue to work on guaranteeing that these measures are put into practice, updated on a regular basis, and available for everyone.

The application of artificial intelligence in cybersecurity adds new benefits as well as new difficulties. Although AI helps improve the detection and reaction to threats, it can lead to concerns over privacy, discrimination, and wrongful use. For this reason, guidelines and regulations are necessary to keep AI from conflicting with human dignity.

Furthermore, encouraging education and awareness about cybersecurity, along with cooperation around the world, support the development of an inclusive and resilient cyber culture. Best practices from other countries can improve Colombia's strategies and make sure that they respect constitutional and worldwide human rights laws.

In short, cybersecurity focused on society is about much more than digital defense; it is about helping people, ensuring their dignity, and encouraging trust. Being proactive, including all groups, and focusing on ethics will be key to using technology for fairness and people's well-being.

REFERENCES

1. Allahrakha, N. (2023). Balancing cyber-security and privacy: Legal and ethical considerations in the digital age. *Law in the Digital Age*, 2(78), 121. DOI 10.17323/2713-2749.2023.2.78.121(lida.hse.ru)
2. Cavelty, M. D., & Kavanagh, C. (2019). Cybersecurity and human rights. In *Research Handbook on Human Rights and Digital Technology* (pp. 73–93). Edward Elgar Publishing. DOI 10.4337/9781785367724.00012(ResearchGate)
3. Cohen, J. E. (2016). The surveillance-innovation complex: The Irony of the participatory turn. *The Information Society*, 32(2), 71–80. https://doi.org/10.1080/01972243.2016.1130501
4. Floridi, L. (2016). The ontological interpretation of informational privacy. *Ethics and Information Technology*, 18(2), 65–73. https://doi.org/10.1007/s10676-016-9395-z
5. Greenleaf, G. (2018). Global data privacy laws 2017: 120 national data privacy laws, including Indonesia and Turkey. *Privacy Laws & Business International Report*, (145), 10–13.
6. Kuner, C. (2017). The Internet and the global reach of EU law. In M. Cremona & J. Scott (Eds.), *EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law* (pp. 121–141). Oxford University Press.
7. Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. *Big Data & Society*, 3(2), 1–21. https://doi.org/10.1177/2053951716679679

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

8. OECD. (2022). Rights in the digital age: Challenges and ways forward. *OECD Digital Economy Papers*, No. 347. DOI 10.1787/deb707a8-en(OECD)
9. Parmar, H., & Murari, U. K. (2025). Fostering ethical human values, ethics, and dignity in the age of artificial intelligence. In *Human Values, Ethics, and Dignity in the Age of Artificial Intelligence* (pp. 213–230). Springer.
10. Regilme, S. S. F. (2019). The global politics of human rights: From human rights to human dignity? *International Political Science Review*, 40(2), 279–290.
11. Rodríguez-Garavito, C. A. (2015). Radical deprivation on trial: The impact of economic inequality on human rights. *Cambridge University Press*.
12. Stevens, Y. Y., Tessono, C., Malik, M. M., & Malik, S. (2023). AI oversight, accountability and protecting human rights: Comments on Canada's proposed artificial intelligence and data act. *Canadian Journal of Law & Technology*, 21(1), 1–15.
13. Vardanyan, L., Stehlík, V., & Kocharyan, H. (2022). Digital integrity: A foundation for digital rights and the new manifestation of human dignity. *TalTech Journal of European Studies*, 12(1), 159–185. DOI 10.2478/bjes-2022-0008(ResearchGate)
14. Wagner, B., & Vieth, K. (2016). The governance of privacy and data protection in the digital age. *International Data Privacy Law*, 6(3), 200–212. https://doi.org/10.1093/idpl/ipw011
15. Wolff, J. (2024). The role of insurers in shaping international cyber-security norms about cyber-war. *Contemporary Security Policy*, 45(1), 141–170.
16. Yeboah-Ofori, A., & Opoku-Akyea, D. (2022). Mitigating cyber supply chain risks in cyber-physical systems organizational landscape. In *Proceedings of the IEEE International Conference on Cyber Security and Internet of Things (CSIoT)* (pp. 43–48). IEEE.
17. Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, 30(1), 75–89. https://doi.org/10.1057/jit.2015.5
18. De Hert, P., & Gutwirth, S. (2018). Data protection in the case law of Strasbourg and Luxembourg: Constitutionalisation in action. In S. Gutwirth, R. Leenes, & P. De Hert (Eds.), *Reloading Data Protection* (pp. 3–44). Springer.
19. Floridi, L., & Taddeo, M. (2016). What is data ethics? *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 374(2083), 20160360. https://doi.org/10.1098/rsta.2016.0360
20. Mokander, J., & Floridi, L. (2021). Ethics-based auditing to develop trustworthy AI. *arXiv preprint arXiv:2105.00002*. https://arxiv.org/abs/2105.00002